Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

Description

All of the CVEs covered in this advisory apply to affected platforms running Arista EOS with the Seamless Bidirectional Forwarding Detection (S-BFD) feature configured.

These issues were discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

CVE-2026-121294

On affected platforms running Arista EOS with a S-BFD reflector proxy configured, an unauthenticated attacker could send a crafted S-BFD Protocol Data Unit (PDU) that might cause the device to temporarily cease reflecting S-BFD packets, potentially resulting in S-BFD session timeouts.

CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CVSSv4.0 Base Score: 6.9
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-1284: Improper Validation of Specified Quantity in Input
This vulnerability is being tracked by BUG 1964292

CVE-2026-121295

On affected platforms running Arista EOS configured as S-BFD peers, an unauthenticated attacker could send a crafted S-BFD PDU to an initiator device. This crafted PDU could cause the kernel on the initiator device to crash, resulting in an unexpected device reboot.

CVSSv3.1 Base Score: 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)
CVSSv4.0 Base Score: 9.2
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-1284: Improper Validation of Specified Quantity in Input
This vulnerability is being tracked by BUG 1966375

Vulnerability Assessment

Platform and Software Applicability Note

To determine actual exposure, operators should first check their software versions against the

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

"Affected Software" list below. If your software release is not listed, your deployment is not vulnerable, regardless of the hardware platform in use.

Affected Software

CVE-2026-121294

EOS Versions

- 4.36.2F and below releases in the 4.36.x train
- 4.35.6M and below releases in the 4.35.x train
- 4.34.8M and below releases in the 4.34.x train
- 4.33.10M and below releases in the 4.33.x train
- All releases in the 4.32.x train
- All releases in the End of Support software in 4.31.x, 4.30.x, 4.29.x trains
- 4.28.2F and later in the End of Support software in the 4.28.x train

CVE-2026-121295

EOS Versions

- 4.36.2F and below releases in the 4.36.x train
- 4.35.6M and below releases in the 4.35.x train
- 4.34.8M and below releases in the 4.34.x train
- 4.33.10M and below releases in the 4.33.x train
- All releases in the 4.32.x train
- All releases in the End of Support software in 4.31.x, 4.30.x, 4.29.x trains

Affected Platforms

The following products **are** affected by this vulnerability:

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010TX Series
  - 7020R/R4 Series
  - 7280R/R2/R3/R4 Series
  - 7500R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 Series
  - CloudEOS
  - cEOS-lab

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products:
    - AWE 5000 Series
    - AWE 7200R Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7130 Series running EOS
    - 7170 Series
    - 7050X3/X4 Series
    - 7060X/X2/X4/X5/X6/XE7 Series
    - 7260X/X3 Series
- Arista Wireless Access Points
- CloudVision CUE cloud service delivery
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- DANZ Monitoring Fabric (DMF) - Controller Appliance
- DANZ Monitoring Fabric (DMF) - Analytics Node Appliance
- DANZ Monitoring Fabric (DMF) - Recorder Node Appliance
- DANZ Monitoring Fabric (DMF) - Service Node Appliance
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
- Arista Multi Cloud Director (formerly Big Switch MCD)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Required Configuration for Exploitation

CVE-2026-121294

In order to be vulnerable to CVE-2026-121294, the following condition must be met:

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

The S-BFD reflector proxy must be enabled. To check whether this configuration is active, run the following command:

```
switch#show running-config section sbfd
router bfd
   sbfd
      reflector local-discriminator <DISC> proxy
```

If the output includes a reflector local-discriminator command with the proxy keyword, the device is exposed to this issue. If the proxy keyword is absent, or if no S-BFD reflector is configured, the device is not exposed to this issue.

CVE-2026-121295

In order to be vulnerable to CVE-2026-121295, the following condition must be met:

The S-BFD initiator round-trip delay measurement feature must be enabled. To confirm whether this configuration is active, run the following command:

```
switch#show running-config section sbfd
router bfd
   sbfd
      initiator measurement delay round-trip
```

If the output includes the initiator measurement delay round-trip command, the device is exposed to this issue. If this command is absent, the device is not exposed to this issue.

Indicators of Compromise

No indicators of compromise exist for both the issues.

Mitigation

No mitigation is available for both the issues.

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below. For more information about upgrading see EOS User Manual: Upgrades and Downgrades

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

CVE-2026-121294 and CVE-2026-121295 has been fixed in the following releases:

- 4.37.0F and later releases in the 4.37.x train
- 4.36.3M and later releases in the 4.36.x train
- 4.35.7M and later releases in the 4.35.x train
- 4.34.9M and later releases in the 4.34.x train
- 4.33.11M and later releases in the 4.33.x train

Hotfix

No hotfix available for this issue.

For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

- Open a Service Request
- By email: support@arista.com
- By telephone: List of regional telephone numbers

Receive notification for new advisories and notices:

Subscribe to the RSS feed and email notifications to receive periodic updates on new software releases, advisories, end of sale and field notices.

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.